

THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

APPLICATION FOR SEARCH WARRANT )  
FOR E-MAIL ACCOUNT )  
[REDACTED]@GMAIL.COM )  
MAINTAINED ON COMPUTER SERVERS )  
OPERATED BY GOOGLE, INC., )  
HEADQUARTERED AT )  
1600 AMPHITHEATRE PARKWAY, )  
MOUNTAIN VIEW, CA )

M-9.  
Misc. No.: 10-291-M-01

UNDER SEAL

AFFIDAVIT IN SUPPORT OF  
APPLICATION FOR SEARCH WARRANT

I, Reginald B. Reyes, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") assigned to the Washington Field Office, and have been employed by the FBI for over five years. I am assigned to a squad responsible for counterespionage matters and matters involving the unauthorized disclosure of classified information, and have worked in this field since October 2005. As a result of my involvement in espionage investigations and investigations involving the unauthorized disclosure of classified information, I am familiar with the tactics, methods, and techniques of particular United States persons who possess, or have possessed a United States government security clearance and may choose to harm the United States by misusing their access to classified information. Before working for the FBI, I was a Special Agent with the Drug Enforcement Administration for two years.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

The statements in this affidavit are based in part on information provided by the investigation to date and on my experience and background as a Special Agent of the FBI. The information set forth in this affidavit concerning the investigation at issue is known to me as a result of my own involvement in that investigation or has been provided to me by other law enforcement professionals. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

3. This affidavit is made in support of an application for a warrant pursuant to 18 U.S.C. § 2703 and 42 U.S.C. § 2000aa to compel Google, Incorporated, which functions as an electronic communication service and remote computing service, and is a provider of electronic communication and remote computing services (hereinafter "Google" or the "PROVIDER"), located at 1600 Amphitheatre Parkway, Mountain View, California, to provide subscriber information, records, and the contents of limited wire and electronic communications pertaining to the account identified as [REDACTED]@gmail.com, herein referred to as the SUBJECT ACCOUNT. I have been informed by the United States Attorney's Office that because this Court has jurisdiction over the offense under investigation, it may issue the warrant to compel the PROVIDER pursuant to 18 U.S.C. § 2703(a).<sup>1</sup>

4. The SUBJECT ACCOUNT is an e-mail account. As discussed below, investigation into the SUBJECT ACCOUNT indicates it is an e-mail account used by a national news reporter (hereinafter "the Reporter").

---

<sup>1</sup> See 18 U.S.C. § 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation . . .").

5. For the reasons set forth below, I believe there is probable cause to conclude that the contents of the wire and electronic communications pertaining to the SUBJECT ACCOUNT, are evidence, fruits and instrumentalities of criminal violations of 18 U.S.C. § 793 (Unauthorized Disclosure of National Defense Information), and that there is probable cause to believe that the Reporter has committed or is committing a violation of section 793(d), as an aider and abettor and/or co-conspirator, to which the materials relate.

6. Based on my training and experience, and discussions with the United States Attorney's Office, I have learned that Title 18, United States Code, Section 793(d) makes punishable, by up to ten years imprisonment, the willful communication, delivery or transmission of documents and information related to the national defense to someone not entitled to receive them by one with lawful access or possession of the same. Specifically, section 793(d) states:

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years or both.

18 U.S.C. § 793(d). Further, section 793(g) makes a conspiracy to violate section 793(d) a violation of 793 and punishable by up to ten years imprisonment. See 18 U.S.C. § 793(g).

7. Based on my training and experience, and discussion with the United States

Attorney's Office, I have learned that "classified" information is defined by Executive Order 12958, as amended by Executive Order 13292, and their predecessor orders, Executive Orders 12356 and 12065, as information in any form that: (1) is owned by, produced by or for, or under control of the United States government; (2) falls within one or more of the categories set forth in the Order; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such damage could reasonably result in "exceptionally grave" damage to the national security, the information may be classified as "TOP SECRET." Access to classified information at any level may be further restricted through compartmentalization "SENSITIVE COMPARTMENTED INFORMATION" (SCI) categories, which further restricts the dissemination and handling of the information.

8. Based on my training and experience, and discussions with the United States Attorney's Office, I have learned that the Privacy Protection Act (the "PPA"), codified at 42 U.S.C. § 2000aa et seq., defines when a search warrant impacting media-related work product and documentary materials may be executed. Section 2000aa(a) of the PPA states, in pertinent part:

**(a) Work product materials**

Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize any *work product materials*<sup>2</sup> possessed by a person reasonably

---

<sup>2</sup> Section 2000aa-7(b) defines the terms "documentary materials" as follows:

(b) "Work product materials", as used in this chapter, means materials, other than contraband or the fruits of a crime or things otherwise criminally possessed, or property designed or intended for use, or which is or has been used, as a means of committing a criminal offense, and –

believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce; but this provision shall not impair or affect the ability of any government officer or employee, pursuant to otherwise applicable law, to search for or seize such materials, if—

- (1) there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate: Provided, however, That a government officer or employee may not search for or seize such materials under the provisions of this paragraph if the offense to which the materials relate consists of the receipt, possession, communication, or withholding of such materials or the information contained therein (but such a search or seizure may be conducted under the provisions of this paragraph if the offense consists of the receipt, possession, or communication of information relating to the national defense, classified information, or restricted data under the provisions of section 793, 794, 797, or 798 of *title 18*, or [other enumerated statutes]) ....

**(b) Other documents**

Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize *documentary materials, other than work product materials*,<sup>3</sup> possessed

- 
- (1) in anticipation of communicating such materials to the public, are prepared, produced, authored, or created, whether by the person in possession of the materials or by any other person;
  - (2) are possessed for the purposes of communicating such materials to the public; and
  - (3) include mental impressions, conclusions, opinions, or theories of the person who prepared, produced, authored or created such material.

42 U.S.C. § 2000aa-7(b).

<sup>3</sup> Section 2000aa-7(a) defines the terms “documentary materials” as follows:

- (a) “Documentary materials”, as used in this chapter, means materials upon which information is recorded, and includes, but is not limited to, written or printed materials, photographs, motion picture films, negatives, video tapes, audio tapes, and other mechanically, magnetically or electronically recorded cards, tapes, or discs, but does not include contraband or fruits of a crime or things otherwise criminally possessed, or property designed or intended for use, or

by a person in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce; but this provision shall not impair or affect the ability of any government officer or employee, pursuant to otherwise applicable law, to search for or seize such materials, if—

- (1) there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate: Provided, however, That a government officer or employee may not search for or seize such materials under the provisions of this paragraph if the offense to which the materials relate consists of the receipt, possession, communication, or withholding of such materials or the information contained therein (but such a search or seizure may be conducted under the provisions of this paragraph if the offense consists of the receipt, possession, or communication of information relating to the national defense, classified information, or restricted data under the provisions of section 793, 794, 797, or 798 of *title 18*, or [other enumerated statutes]) ...

42 U.S.C. § 2000aa(a) (emphasis added). Thus, section 2000aa(a) specifically exempts from its prohibitions cases in which there is probable cause to believe that the possessor of media related work product or documentary materials has committed a violation of section 793. I have been further informed that the legislative history of the statute indicates:

The purpose of the statute is to limit searches for materials held by persons involved in First Amendment activities who are themselves not suspected of participation in the criminal activity for which the materials are sought, and not to limit the ability of law enforcement officers to search for and seize materials held by those suspected of committing the crime under investigation.

S. Rep. No. 96-874 at 11 (1980), reprinted in 1980 U.S.C.C.A.N. 3950. I also have been informed that violations of the PPA do not result in suppression of the evidence, see 42 U.S.C. §

---

which is or has been used as, the means of committing a criminal offense.

42 U.S.C. § 2000aa-7(a).

2000aa-6(d), but can result in civil damages against the sovereign whose officers or employees executed the search in violation of section 2000aa(a). See 42 U.S.C. § 2000aa-6(a).

## **II. FACTS SUPPORTING PROBABLE CAUSE**

9. In or about June 2009, classified United States national defense information was published in an article on a national news organization's website (hereinafter the "June 2009 article"). The June 2009 article was written by the Reporter who frequently physically worked out of a booth located at the main Department of State (DoS) building located at 2201 C Street, N.W., Washington, D.C.

10. The Intelligence Community owner of the classified information at issue (the "Owner") has informed the FBI that the June 2009 article disclosed national defense information that was classified TOP SECRET/SPECIAL COMPARTMENTED INFORMATION (TS/SCI). It has also informed the FBI that the information was not declassified prior to its disclosure in the June 2009 article, that the information's public disclosure has never been lawfully authorized, and that the information remains classified at the TS/SCI level to this day.

11. Following the disclosure of the classified national defense information in the June 2009 article, an FBI investigation was initiated to determine the source(s) of the unauthorized disclosure. That investigation has revealed that the Owner's TS/SCI information disclosed in the June 2009 article was first made available to a limited number of Intelligence Community members in an intelligence report (the "Intelligence Report") that was electronically disseminated to the Intelligence Community outside of the Owner on the morning of the date of

publication of the June 2009 article. The Intelligence Report was accessible on a classified information database that warned all Intelligence Community users seeking access to information in the database, through a "click through" banner, of the following:

Due to recent unauthorized disclosures of sensitive intelligence, you are reminded of your responsibility to protect the extremely sensitive, compartmented intelligence contained in this system. Use of this computer system constitutes consent to monitoring of your actions. None of the intelligence contained in this system may be discussed or shared with individuals who are not authorized to receive it. Unauthorized use . . . is prohibited and violations may result in disciplinary action or criminal prosecution.

12. The Intelligence Report was clearly marked TS/SCI. The security markings further instructed the reader that every portion of the information contained in the Intelligence Report was classified TS/SCI and was not authorized for disclosure without permission of the Owner.

13. The investigation has revealed that one individual who accessed the Intelligence Report through the classified database on the date of the June 2009 article (prior to the publication of the article) was Stephen Jin-Woo Kim.<sup>4</sup> Review of government records has revealed that Mr. Kim was born on [REDACTED] and was naturalized as a United States

---

<sup>4</sup> So far, the FBI's investigation has revealed in excess of 95 individuals, in addition to Mr. Kim, who accessed the Intelligence Report on the date of the June 2009 article and prior to its publication. To date, however, the FBI's investigation has not revealed any other individual, other than Mr. Kim, who both accessed the Intelligence Report and who also had contact with the Reporter on the date of publication of the June 2009 article. Thus far, the FBI's investigation has revealed four other individuals who have admitted to limited contacts with either the Reporter's news organization or the Reporter anywhere from six weeks, to six months, or to nine years prior to publication of the June 2009 article. The FBI's investigation of these contacts is on-going. All these individuals have denied being the source of the June 2009 article and the FBI has not discovered any information to date that would tend to discredit their statements.



citizen in 1988.<sup>5</sup> Mr. Kim is a Lawrence Livermore National Laboratory employee who was on detail to the DoS's Bureau of Verification, Compliance, and Implementation (VCI) at the time of the publication of the June 2009 article. VCI is responsible for ensuring that appropriate verification requirements are fully considered and properly integrated into arms control, nonproliferation, and disarmament agreements and to monitor other countries' compliance with such agreements. On his detail to VCI, Mr. Kim worked as a Senior Advisor for Intelligence to the Assistant Secretary of State for VCI.

14. Like the Reporter's booth at DoS on the date of publication of the June 2009 article, Mr. Kim's VCI office was located at the DoS headquarters building at 2201 C Street, N.W., Washington, D.C.

15. Based on my training and experience, I have learned that classified information, of any designation, may be shared only with persons determined by an appropriate United States government official to be eligible for access to classified information, that is, the individual has received a security clearance, has signed an approved non-disclosure agreement and possesses a "need to know" the information in question. If a person is not eligible to receive classified information, classified information may not be disclosed to that person.

16. Government records demonstrate that, at all times relevant to this investigation, Mr. Kim possessed a TS/SCI security clearance. As a government employee with a security clearance, and prior to the disclosures at issue, Mr. Kim executed multiple SF 312 Classified Information Non-Disclosure Agreements (NDAs) with the Government. NDAs are legally

---

<sup>5</sup> In prior affidavits in this matter seeking search warrants of Mr. Kim's e-mail accounts, the date of Mr. Kim's naturalization was erroneously reported as 1999 rather than 1988.

binding agreements between an individual being granted, or already in possession of, a security clearance, and the United States Government wherein the parties agree that the individual never disclose classified information without the authorization of the Government. The NDAs further notified Mr. Kim that the unauthorized disclosure of classified information can lead to criminal prosecution, including for violations of 18 U.S.C. § 793.

17. The Reporter did not possess a security clearance and was not entitled to receive the information published in the June 2009 article. Nor was Mr. Kim authorized, directly or indirectly, by the United States Government to deliver, communicate, or transmit the TS/SCI information in the article to the Reporter or any other member of the press.

18. Government electronic records revealed that between the hours the Intelligence Report was made available to the Intelligence Community on the morning of the publication of the June 2009 article, and the publication of the June 2009 article, the unique electronic user profile and password associated with Mr. Kim *accessed at least three times* the Intelligence Report that contained the TS/SCI information which later that day was disclosed in the June 2009 article.<sup>6</sup> Specifically, the Intelligence Report was accessed by Mr. Kim's user profile at or

---

<sup>6</sup> Mr. Kim accessed the classified database in question through his DoS work computer provided to him to process and access TOP SECRET/SCI information. The "click through" banner on Mr. Kim's DoS classified computer permits the government's review of the data contained therein. It read:

**NOTICE AND CONSENT LOG-ON BANNER**

**THIS IS A DEPARTMENT OF STATE (DoS) COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS, AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DoS COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED**

around 11:27 a.m., 11:37 a.m., and 11:48 a.m. on the date the article was published. DoS security badge access records suggest that, at those times, Mr. Kim was in his VCI office suite where his DoS TS/SCI computer was located on which he would have accessed the Intelligence Report.

19. Telephone call records demonstrate that earlier on that same day, multiple telephone communications occurred between phone numbers associated with Mr. Kim and with the Reporter. Specifically:

- at or around 10:15 a.m., an approximate 34-second call was made from the Reporter's DoS desk telephone to Mr. Kim's DoS desk telephone;
- two minutes later, at or around 10:17 a.m., an approximate 11 minute 35 second call was made from Mr. Kim's DoS desk telephone to the Reporter's DoS desk telephone;

---

ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DoS ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DoS COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

Further, Mr. Kim had to "click through" *an additional* banner on the classified database where he accessed the Intelligence Report, as detailed in Paragraph 11 above, which stated that "use of this computer system constitutes consent to monitoring of your actions."

Moreover, DoS policy specifically prescribes that "personal use [of DoS classified computers] is strictly prohibited; therefore, users do not have a reasonable expectation of privacy." 12 FAM 632.1.5; 5 FAM 723(2). In addition, the DoS's Foreign Affairs Manual states that DoS office spaces are subject to security inspections to insure that classified information is properly protected. Indeed, Mr. Kim's office was located in a secured facility within the main DoS building that was subject to daily inspections by rotating duty officers (sometimes including Mr. Kim himself) who were responsible for making sure that classified information in each of the offices within the facility was properly secured.

- one hour later, at or around 11:18 a.m., an approximate 3 minute 58 second call was made from Mr. Kim's DoS desk telephone to the Reporter's DoS desk telephone; and
- at or around 11:24 a.m., an approximate 18 second call was made from Mr. Kim's DoS desk telephone to the Reporter's DoS desk telephone.

20. Thereafter, telephone call records for Mr. Kim's office phone reveal that *at or around the same time that Mr. Kim's user profile was viewing the TS/SCI Intelligence Report two telephone calls were placed from his desk phone to the Reporter.* Specifically, a call was made at or around 11:37 a.m (at or around the same time that Mr. Kim's user profile was viewing the Intelligence Report) from Mr. Kim's desk phone to the Reporter's desk phone located within the DoS. That call lasted approximately 20 seconds. Immediately thereafter, a call was placed by Mr. Kim's desk phone to the Reporter's cell phone. This second call lasted approximately 1 minute and 8 seconds.

21. In the hour following those calls, the FBI's investigation has revealed evidence suggesting that Mr. Kim met face-to-face with the Reporter outside of the DoS. Specifically, DoS security badge access records demonstrate that Mr. Kim and the Reporter departed the DoS building at 2201 C Street, N.W., at nearly the same time, they were absent from the building for nearly 25 minutes, and then they returned to the DoS building at nearly the same time. Specifically, the security badge access records indicate:

- Mr. Kim departed DoS at or around 12:02 p.m. followed shortly thereafter by The Reporter at or around 12:03 p.m.; and
- Mr. Kim returned to DoS at or around 12:26 p.m. followed shortly thereafter by The Reporter at or around 12:30 p.m.

22. Within a few hours after those nearly simultaneous exits and entries at DoS, the

June 2009 article was published on the Internet. Following the publication of the article, yet another call was placed from Mr. Kim's DoS desk telephone to the Reporter's DoS desk telephone number. This call lasted approximately 22 seconds.

23. In the evening of August 31, 2009, DoS Diplomatic Security entered Mr. Kim's DoS office space, without his knowledge, pursuant to DoS internal regulations, procedures, and computer banner authority for purposes of imaging his computer hard drives. Lying in plain view on Mr. Kim's desk next to his DoS computer was a photocopy of the June 2009 article as well as two other articles published in June 2009. All three articles were stapled together. These three articles were also observed on Mr. Kim's desk during entries made in his DoS office space on September 21 and 22, 2009.

24. On September 24, 2009, the FBI conducted a non-custodial interview of Mr. Kim concerning the leak of classified information in the June 2009 article, among other leaks of classified information. During that interview, Mr. Kim denied being a source of the classified information in the June 2009 article. Mr. Kim also claimed to have no recollection of one of the other two articles which were seen in plain view on his desk on August 31, 2009. Mr. Kim admitted to meeting the Reporter in approximately March 2009 but denied having any contact with the Reporter since that time. Mr. Kim acknowledged that DoS protocol required that he would have to go through the DoS press office before he could speak with the press. Mr. Kim stated, "I wouldn't pick-up a phone and call [the Reporter] or [the news organization that the Reporter works for]."

25. An analysis of call records for Mr. Kim's DoS *desk phone* reveals that between May 26, 2009 and July 14, 2009, *36 calls* were placed to or received from telephone numbers

associated with the Reporter, including the 7 aforementioned calls on the date of the publication of the June 2009 article. Further, there were 3 *calls* during this timeframe between his desk phone and a number associated with the Reporter's news organization.

26. During the September 24, 2009 non-custodial interview, when asked by the FBI for a cell phone number to reach him in the future, Mr. Kim stated that his cell phone was "no longer active" as of the day of the interview. Mr. Kim indicated to the FBI that he would be purchasing a new cell phone with a different number.

27. An analysis of call records for Mr. Kim's *cellular phone* reveals that between May 26, 2009 and June 30, 2009, 16 *calls* were placed to or received from telephone numbers associated with the Reporter and 10 *calls*<sup>7</sup> were placed to or received from telephone numbers associated with the Reporter's news organization.

28. It is apparent from the foregoing both that Mr. Kim was in contact with the Reporter on multiple occasions prior to and after the publication of the June 2009 article, and that Mr. Kim did not want the FBI, who he knew was investigating the leak of classified information in that article, to know about those contacts. The FBI has also learned that, following its interview with Mr. Kim, he provided the Department of Energy (DoE) – for which Mr. Kim's permanent employer, LLNL, is a sub-contractor – with "pre-paid" cell phone number

---

<sup>7</sup> In prior affidavits in this matter seeking search warrants of Mr. Kim's e-mail accounts, it was reported that there were 11 calls between Mr. Kim's cellular phone and telephone numbers associated with the Reporter's news organization. Mr. Kim's toll records for his cellular phone do, in fact, list 11 such calls. Further review of those records suggested, however, that one of the calls may have been double counted by Mr. Kim's cellular telephone service provider. Discovering this discrepancy, the service provider was contacted and indicated that what appears to be two calls on the toll records was, in fact, only a single call. Accordingly, in this affidavit, I have corrected the total of the calls between Mr. Kim's cellular telephone and telephone numbers associated with the Reporter's news organization to reflect that there were only 10 such calls.

(sometimes referred to as a "throw away" phone) that he instructed DoE representatives to use in the future to contact him about future employment opportunities.

29. Similarly, during the same September 24, 2009 non-custodial interview, Mr. Kim told the FBI that the best e-mail address through which to contact him was [REDACTED]@yahoo.com. One day later, Mr. Kim e-mailed the FBI and stated that "[m]y yahoo account that I gave you is full and am [sic] going to get rid of it. I can be reached at [REDACTED]@gmail.com." It is apparent from the foregoing that, like his cell phone number, Mr. Kim was concerned about the FBI focusing on his [REDACTED]@yahoo.com e-mail account.

30. Following the FBI's interview of Mr. Kim on September 24, 2009, FBI and DoS/Diplomatic Security entered Mr. Kim's office on the evening of September 26, 2009. The stapled photocopies of the three articles containing classified information (including the June 2009 article) seen next to Mr. Kim's computer on August 31, 2009, September 21 and 22, 2009, were no longer present in Mr. Kim's office on September 26<sup>th</sup> – two days after his interview with the FBI wherein he was questioned about the unauthorized disclosures of classified information in the June 2009 article.

31. A forensic analysis of the hard drive imaged from Mr. Kim's DoS unclassified DoS computer,<sup>8</sup> has revealed an e-mail communication, dated July 11, 2009, from the Reporter's

---

<sup>8</sup> The "click through" banner on Mr. Kim's DoS unclassified computer permits the government's review of the data contained therein. It reads as follows:

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to the network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

---

Unauthorized or improper use of this system may result in disciplinary actions, as well as civil and criminal penalties.

By using this information system, you understand and consent to the following:

- \* You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.
- \* Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.

Nothing herein consents to the search and seizure of a privately-owned computer or other privately owned communications device, or the contents thereof, that is in the system user's home.

Further, when he first started at the DoS in June 2008, Mr. Kim signed an "Internet Briefing Acknowledgement" and "Security Briefing for OpenNet+ Account" forms, both of which stated that he understood that his use of Government provided Internet and of his OpenNet+ account "may be monitored at any time." He also signed a "Waiver Statement Form," wherein he acknowledged that he understood that

- he did "not have a reasonable expectation of privacy concerning the data on [his] computer;"
- "All data contained on [his] computer may be monitored, intercepted, recorded, read, copied, or captured in any manner by authorized personnel. For example supervisors, system personnel or security personnel may give law enforcement officials any potential evidence of crime, fraud, or employee misconduct found on [his] computer."
- "Law enforcement may be authorized to access and collect evidence from [his] computer."
- "Authorized personnel will be routinely monitoring [his] computer for authorized purposes."
- "Consequently, any use of [his] computer by any user, authorized or unauthorized, constitutes DIRECT CONSENT to monitoring of [his] computer."

Similarly, while DoS policy permits limited personal use of the Internet and personal e-mail through an Internet connection, that policy also states:

Employees have no expectation of privacy while using any U.S. Government-provided access to



e-mail account to an e-mail account entitled [REDACTED]@yahoo.com. The e-mail from the Reporter forwarded another e-mail from other news reporters which included in its body a news article (not written by the Reporter) that would appear in the Washington Times (not the Reporter's news organization) the following day, July 12, 2009. This e-mail was found in the unallocated space located on Mr. Kim's DoS unclassified hard drive. I have been informed that when a computer file is deleted, the deleted file is flagged by the operating system as no longer needed, but remains on the hard disk drive in unallocated space unless the data is later overwritten.

32. Electronic evidence retrieved from Mr. Kim's DoS unclassified workstation also revealed that on September 24, 2009, following his interview with the FBI, Mr. Kim's user profile logged into the [REDACTED]@yahoo.com account through an DoS Internet connection accessed through his DoS unclassified workstation. DoS security badge access records suggest that Mr. Kim was in his VCI office suite where his DoS unclassified workstation was located when the [REDACTED]@yahoo.com account was accessed on September 24, 2009. While accessing that account on his DoS computer, Mr. Kim's user profile observed e-mails in that account from an e-mail account entitled [REDACTED]@gmail.com (which is the subject matter of the Government's request for a warrant here). Mr. Kim's profile also observed e-mails between the Reporter's work e-mail and [REDACTED]@yahoo.com, the e-mail account

---

the Internet. The Department considers electronic mail messages on U.S. Government computers, using the Internet or other networks, to be government materials and it may have access to those messages whenever it has a legitimate purpose for doing so. Such messages are subject to regulations and laws covering government records, and may be subject to Freedom of Information Act (FOIA) request or legal discovery orders."

identified by Mr. Kim as his own during his September 24, 2009 interview with the FBI, but which, one day later, he told the FBI was "full" and that he was "going to get rid of it."

33. During the Internet session described above on September 24, 2009, Mr. Kim attempted to clear his "Temporary Internet Files." I have been informed that deletion of Temporary Internet Files created by a web browser software application moves the cached content of internet sites visited to unallocated space, which, again, is space on the hard drive flagged by the operating system as being available for overwriting.

34. On November 9, 2009, search warrants were executed on both the [REDACTED]@yahoo.com and [REDACTED]@yahoo.com e-mail accounts. Those searches revealed multiple e-mails between Mr. Kim and the Reporter dating between May 11, 2009 and August 15, 2009. Review of those e-mails demonstrates that [REDACTED]@yahoo.com and [REDACTED]@yahoo.com are e-mail accounts used by Mr. Kim and [REDACTED]@gmail.com is an account used by the Reporter<sup>9</sup> to receive e-mails from Mr. Kim and perhaps other sources. Further, in their e-mail communication, Mr. Kim and the Reporter appear to have employed aliases (i.e., Mr. Kim is "Leo" and the Reporter is "Alex"). The content of the e-mail communications also demonstrate that Mr. Kim was a source for the Reporter concerning the foreign country that was the subject matter of the June 2009 article (the "Foreign Country") and that the Reporter solicited the disclosure of intelligence information from Mr. Kim concerning that country. A chronological listing and description of the most

---

<sup>9</sup> "[REDACTED]" is not the name of the Reporter. Rather, this e-mail account was apparently named after a former Deputy Assistant to President Richard Nixon who is best known as the individual responsible for the secret taping system installed in the Nixon White House, and who exposed the existence of that taping system when he testified before Congress during the Watergate hearings.

pertinent e-mails is as follows:

- (a). A May 11, 2009 e-mail from [REDACTED]@yahoo.com to [REDACTED]@gmail.com reads:

I am back from my trip. Here is my personal information.

Please send me your personal cell number. I believe you have mine. It was great meeting you.

Thanks,

Stephen

(Mr. Kim attached to this e-mail his resume and a biographical description, both of which noted his access to classified information and his expertise concerning the Foreign Country).

- (b). A May 20, 2009 e-mail from [REDACTED]@gmail.com to [REDACTED]@yahoo.com responding to the above May 11, 2009 e-mail outlines a clandestine communications plan between Mr. Kim and the Reporter. In the e-mail, the Reporter solicits Mr. Kim as a source of sensitive and/or internal government documents (*italicized below*). It reads:

Your credentials have never been doubted – but I am nonetheless grateful to have the benefit of a chronological listing of your postings and accomplishments. I only have one cell phone number, on my Blackberry, which I gave you 202-[phone number for the Reporter]. Unfortunately, when I am seated in my booth at the State Department, which is much of every day, it does not get reception. thus [sic] I instruct individuals who wish to contact me simply to send me an e-mail to this address [REDACTED]@gmail.com]. *One asterisk means to contact them, or that previously suggested plans for communication are to proceed as agreed; two asterisks means the opposite.* With all this established, and presuming you have read/seen enough about me to know that I am trustworthy . . . let's get about our work! What do you want to accomplish together? As I told you when we met, I can always go on television and say: "Sources tell [name of the Reporter's national news organization]" But I am in a much better position to advance the interests of all concerned if I can say: "[Name of the Reporter's national news organization] has obtained . . ."

Warmest regards, [first name of Reporter].

[Emphasis added]

- (c). Another May 20, 2009 e-mail from [REDACTED]@gmail.com to [REDACTED]@yahoo.com, the body of which states:

Please forgive my delay in replying to you. I was on vacation out of town

....

Yours faithfully, [first name of Reporter]

- (d). A May 22, 2009 e-mail from [REDACTED]@gmail.com to [REDACTED]@yahoo.com in which the Reporter explicitly seeks from Mr. Kim the disclosure of intelligence information about the Foreign Country. It reads:

Thanks Leo. What I am interested in, as you might expect, is breaking news ahead of my competitors. I want to report authoritatively, and ahead of my competitors, on new initiatives or shifts in U.S. policy, events on the ground in [the Foreign Country], *what intelligence is picking up*, etc. As possible examples: I'd love to report that the IC<sup>10</sup> *sees activity inside* [the Foreign Country] suggesting [description of national defense information that is the subject of the intelligence disclosed in the June 2009 article]. I'd love to report on what the hell [a named U.S. diplomat with responsibilities for the Foreign Country] is doing, maybe on the *basis of internal memos* detailing how the U.S. plans to [take a certain action related to the Foreign Country] (if that is really our goal). I'd love to see some *internal State Department analyses* about the state of [a particular program within the Foreign Country that was the subject matter of the June 2009 article], about [the leader of the Foreign Country]. . . . In short: Let's break some news, and expose muddle-headed policy when we see it – or force the administration's hand to go in the right direction, if possible. The only way to do this is to EXPOSE the policy, or *what the [Foreign Country] is up to*, and the only way to do that authoritatively is with *EVIDENCE*.

Yours faithfully, Alex.

[Emphasis added]

- (e). Mr. Kim forwarded an e-mail containing the above May 22, 2009 [REDACTED]@gmail.com e-mail to his [REDACTED]@yahoo.com at 10:57

<sup>10</sup> "IC" is a common acronym denoting "Intelligence Community."

a.m. on the date of the June 2009 article. At the time of this e-mail, DoS badge records indicate that Mr. Kim and the Reporter were outside the DoS building, having left the building at approximately the same time. The content of the forwarded e-mail is blank, but the subject line is "Fw: Re: here."

- (f). In an e-mail dated in June 2009, following the publication of the June 2009 article, the Reporter forwarded from the Reporter's work e-mail account (which spells out the Reporter's name) to the [REDACTED]@yahoo.com account the following e-mail from another reporter associated with the Reporter's national news organization. It reads:

Hi [first name of Reporter] – wondering if you would like to check with your sources on something we are hearing but can't get totally nailed down over here.

It seems that the [U.S. Government is concerned about something related to the Foreign Country] and is watching it very closely . . . We can't get many more details than that right now – but our source said if we could find [a specific detail] elsewhere he would give us more. Though you might be able to squeeze out a few details and we could double team this one . . . .

Many thanks, dear friend . . . .,

[Name of second reporter associated with Reporter's national news organization]

The Reporter then forwarded the above e-mail asking for the Reporter to "squeeze out a few details" about the Foreign Country from the Reporter's "sources" to Mr. Kim at his [REDACTED]@yahoo.com account and included the following introductory note:

Leo: From the [Reporter's national news organization] Pentagon correspondent. I am at 202-[Reporter's office number at the Reporter's news organization] today.

Hugs and kisses, Alex<sup>11</sup>

---

<sup>11</sup> One day after this e-mail was sent, toll records indicate that Mr. Kim placed a six-and-a-half minute phone call to the Reporter's office number at the Reporter's news organization (as requested in the above-referenced e-mail).

- (g). An e-mail dated in June 2009 from the Reporter's work e-mail to [REDACTED]@yahoo.com containing a subject referencing the Foreign Country. The content of the e-mail included only the Reporter's phone number next to an asterisk (\*) which, according to the May 20, 2009 e-mail described above, was the Reporter's signal that Mr. Kim should call him.<sup>12</sup>
- (h). A July 11, 2009 e-mail from the Reporter's work e-mail to [REDACTED]@yahoo.com attaching, without comment, a news article *dated the following day* from another national news organization concerning the intelligence community.
- (i). A July 12, 2009 e-mail from the Reporter's work e-mail to [REDACTED]@yahoo.com attaching, without comment, a news article *dated the following day* from another national news organization concerning the Foreign Country.
- (j). An August 15, 2009 e-mail from the [REDACTED]@yahoo.com account to the Reporter's work e-mail account, which states:

Hope you are alright but I sense that they are not.

- (k). An August 15, 2009 e-mail from the Reporter's work e-mail responding to the above e-mail, and stating:

Leo,

You are most perceptive and I appreciate your inquiry. Call me at work on Monday [at the Reporter's work phone number] and I will tell you about my reassignment. In the meantime, enjoy your weekend!

Alex

(The electronic signature to this e-mail following the word "Alex" identifies the Reporter by the Reporter's full name, phone number, e-mail address, and media organization).

35. The FBI conducted a second non-custodial interview of Mr. Kim on March 29,

---

<sup>12</sup> On the date of this e-mail, Mr. Kim was traveling outside of the United States. Mr. Kim's toll records do not indicate that Mr. Kim called the Reporter after this e-mail was sent. They do indicate, however, that three minutes after this e-mail was sent, a 53 second call was placed from a number associated with the Reporter's news organization to Mr. Kim's cell phone.

2010. During the interview Mr. Kim made a number of admissions, including:

- confirming that the Owner's information disclosed in the June 2009 article was national defense information and most of it, in Mr. Kim's mind, was properly classified at the TOP SECRET/SCI level;
- confirming that the same disclosures in the June 2009 article were, in Mr. Kim's mind, "egregious," "bad" and harmful to the national security in a number of respects which he described in detail;
- acknowledging that, while he could not recall the specifics of the Intelligence Report, he was "fairly certain" he had reviewed it and agreed that if electronic records indicated that he had accessed the Report then he did so;
- agreeing that the Owner's information disclosed in the June 2009 article appeared to be derived from the Intelligence Report with only one difference that he described as a "subtle nuance;"
- acknowledging that he had received extensive training on the handling of classified information, and had executed multiple classified information non-disclosure agreements with the Government;
- confirming that he understood the TS/SCI classification markings that were prominently displayed on the Intelligence Report;
- admitting that the Owner's information disclosed in the June 2009 article, to his knowledge, did not "match" information in the public domain, but advising that "bits and pieces" of the article were possibly derived from open source information;
- acknowledging that he understood the security banner on the classified computer database and that his actions were subject to monitoring;
- re-stating his false statement from his interview with the FBI on September 24, 2009, that he had no contact with the Reporter after they first met in March 2009;
- after being confronted with the evidence of his extensive contacts with the Reporter in the months after they first met, (i) first stating that his calls with the Reporter had been facilitated by an unidentified "friend" and that he did not inform the FBI of his telephone contacts with the Reporter because he did not consider them "direct contacts;" but then later (ii) openly admitting during the interview that he had "lied" to the FBI about the extent of his relationship with the Reporter because he was "scared" that the FBI might investigate him for the leak;

- while denying that he had met face-to-face with the Reporter on the date of the June 2009 article, admitting that he had met with the Reporter outside of the DoS building at other times including once following the FBI's September 24, 2009 interview;
- admitting that the emails seized during the FBI's investigation were, in fact, emails between himself and the Reporter;
- admitting, after being asked the question a number of times, that "Leo Grace" was an alias used in the e-mails for himself and that "Alex" was an alias used by the Reporter, and
- while asserting that the [REDACTED]@yahoo.com account pre-dated his relationship with the Reporter, stating that it was the Reporter's idea to use covert e-mail communications as a means of compartmentalizing the information and a way for Mr. Kim to "feel comfortable talking with [the Reporter]."

36. According to the FBI agents who conducted the interview, during the interview, Mr. Kim never provided a coherent explanation for the evidence of his extensive contacts with the Reporter including on the date of the leak in question. At one point, he indicated that he was communicating with the Report hoping that the Reporter "could help put him in a think tank." Mr. Kim's reaction to the evidence was mostly stunned silence, although at one point he admitted that some of the evidence was "very disturbing." Nevertheless, Mr. Kim denied that he was a source for the Reporter or had knowingly provided the Reporter with classified documents or information. Mr. Kim claimed to have specifically informed the Reporter that the Reporter "won't get stuff out of me," to which the Reporter allegedly replied, "I don't want anything." Mr. Kim did admit, however, that he may have "inadvertently" confirmed information that he believed the Reporter had already received from other individuals. Mr. Kim made further



statements which could fairly be characterized as either a confession or a near confession<sup>13</sup>:

- “I did not purposely discuss the [Intelligence Report], but might have discussed [some of the topics discussed in the Report].”
- “Maybe I inadvertently confirmed something . . . too stubborn to not . . . [I] just don’t know . . . someone values my views, listens up, . . . maybe I felt flattered. [The Reporter] is a very affable, very convincing, persistent person. . . [The Reporter] would tell me I was brilliant and it is possible I succumbed to flattery without knowing it. Maybe it was my vanity. [The Reporter] considers me an expert and would tell me . . . could use my insight. . . . The IC is a big macho game but I would never say I’m read in to this and you are not. I would never pass [the Reporter] classified.”
- “[The Reporter] exploited my vanity.”
- “[M]y personal and professional training told me not to meet people like [the Reporter]. I felt like while on the phone I was only confirming what he already knew. I was exploited like a rag doll. [The Reporter] asked me a lot of questions and got me to talk to him and have phone conversations with him. [The Reporter] asked me a lot, not just specific countries. [The Reporter] asked me how nuclear weapons worked.”
- “It’s apparent I did it. I didn’t say ‘did you see this?’ I think I did it. I can’t deny it. I didn’t give [the Reporter] the [specific intelligence information in the article]. I didn’t provide him with the stuff.”
- “I don’t think I confirmed . . . maybe I inadvertently confirmed in the context of other conversations [with the Reporter]. It wasn’t far-fetched that the information was out there. I would not talk over an open line about intelligence. I did not leak classified.”
- Finally, Mr. Kim opined that “someone either gave [the Reporter] the [the Intelligence Report] or it was read to [the Reporter] over the telephone.”

37. During his interview, Mr. Kim also consented to a physical search of his condominium in McLean, Virginia. No hard-copy classified documents or other hard-copy materials directly related to the leak at issue were found during the search of Mr. Kim’s

---

<sup>13</sup> The FBI interview was not audio or video taped. What follows are excerpts from an FBI report memorializing the interview.

condominium. During the search the FBI recovered three computers that are presently being analyzed. Thus far, no information relevant to this investigation has been identified on those computers.

38. The text of the June 2009 article reflects the Reporter's knowledge and understanding that the information the Reporter had received was intelligence information the disclosure of which could be harmful to the United States.

39. I conclude from the foregoing that there is probable cause to believe that:

- (a). From the beginning of their relationship, the Reporter asked, solicited and encouraged Mr. Kim to disclose sensitive United States internal documents and intelligence information about the Foreign Country. Indeed, in the May 20, 2009 e-mail, the Reporter solicits from Mr. Kim some of the national defense intelligence information that was later the subject matter of the June 2009 article;
- (b). The Reporter did so by employing flattery and playing to Mr. Kim's vanity and ego;
- (c). Much like an intelligence officer would run an clandestine intelligence source, the Reporter instructed Mr. Kim on a covert communications plan that involved the e-mail of either one or two asterisks to what appears to be a e-mail account set up by the Reporter, [REDACTED]@gmail.com, to facilitate communication with Mr. Kim and perhaps other sources of information;
- (d). To conceal further their communications, the Reporter and Mr. Kim employed aliases in their e-mail communication to each other (i.e., Mr. Kim is "Leo" and the Reporter is "Alex");
- (e). The Reporter was in repeated telephone contact with Mr. Kim prior to, and on the day of, the leak of the classified information in question;
- (f). On the day of the leak, Mr. Kim was on the telephone with the Reporter at or around the same time that Mr. Kim was viewing the Intelligence Report containing TOP SECRET/SCI national defense information about the Foreign Country;
- (g). The text of the June 2009 article reflects the Reporter's knowledge and understanding that the information the Reporter had received was intelligence

information the disclosure of which could be harmful to the United States;

- (h). Nevertheless, the Reporter published an article on the Internet containing the TOP SECRET/SCI national defense information about the Foreign Country that was in the Intelligence Report;
- (i). Thereafter, it appears the Reporter (i) returned the favor by providing Mr. Kim with news articles *in advance of their publication* concerning intelligence matters and the Foreign Country and (ii) continued to contact Mr. Kim as a source when the Reporter's colleagues needed sensitive government information about the Foreign Country.

40. Based on the foregoing, there is probable cause to believe that the Reporter has committed a violation of 18 U.S.C. § 793 (Unauthorized Disclosure of National Defense Information), at the very least, either as an aider, abettor and/or co-conspirator of Mr. Kim.

### **III. ITEMS TO BE SEIZED**

41. Further, based on the foregoing, there is probable cause to believe that evidence material to this investigation will be found in the [REDACTED]@gmail.com account. While the searches of Mr. Kim's e-mail accounts have revealed a number of e-mails between Mr. Kim and the Reporter, certain of those e-mails indicate that there are additional e-mail communications that have not been recovered by the FBI and that, if they still exist, would likely be found in the [REDACTED]@gmail.com account. Specifically, the searches of Mr. Kim's [REDACTED]@yahoo.com e-mail account did not reveal his responses to the May 20, 2009 or May 22, 2009 e-mails from the Reporter soliciting sensitive, internal and/or intelligence information about the Foreign Country. The May 22, 2009 e-mail from the Reporter, for example, begins "Thanks Leo. What I am interested in, as you might expect, is breaking news ahead of my competitors." Thus, the May 22nd e-mail is a response from the Reporter to an earlier e-mail from Mr. Kim apparently inquiring as to what kind of information the Reporter

response to this warrant:

- (i) all communications, on whatever date, between [REDACTED]@gmail.com and Mr. Kim's known e-mail accounts, i.e., [REDACTED]@yahoo.com, [REDACTED]@yahoo.com, and [REDACTED]@gmail.com;<sup>14</sup> and
- (ii) all communications "to" or "from" the [REDACTED]@gmail.com on June 10<sup>th</sup> and 11<sup>th</sup>, 2009.

45. While it is not required for a warrant to issue under section 2000aa, the FBI has exhausted all reasonable non-media alternatives for collecting the evidence it seeks. We seek e-mails between the Reporter and Mr. Kim that we have probable cause to believe existed. To gather that evidence, we have the option of searching either the Reporter's or Mr. Kim's e-mail accounts. Our searched of Mr. Kim's e-mail accounts have not yielded all the e-mails between him and the Reporter that our evidence to date demonstrates exist. Other than asking the Reporter for a voluntary production of the e-mails from the [REDACTED]@gmail.com account, there is no other way to get the evidence we rightfully seek. Because of the Reporter's own potential criminal liability in this matter, we believe that requesting the voluntary production of the materials from Reporter would be futile and would pose a substantial threat to the integrity of the investigation and of the evidence we seek to obtain by the warrant.

46. Based on the above, there is probable cause to believe that the Reporter (along with Mr. Kim) has committed a violation of 18 U.S.C. § 793(d) either as Mr. Kim's co-conspirator and/or aider and abettor, and that evidence of that crime is likely contained within the [REDACTED]@gmail.com account. Accordingly, the FBI's request to search the contents of

---

<sup>14</sup> A Google representative has indicated that, if ordered by a court as part of a search warrant, Google can produce e-mail communications between certain e-mail accounts.

that account falls squarely within section 2000aa(a)'s exception permitting searches of media-related work product materials, even when possessed by a national news reporter because there is "probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate." 42 U.S.C. § 2000aa(a).

47. On October 2, 2009, the FBI submitted a preservation letter to Google, pursuant to 18 U.S.C. § 2703(f), requesting that the contents of [REDACTED]@gmail.com be preserved. On January 15, 2010, a second preservation letter for the account was sent to Google. This second preservation letter was 15 days over the 90-day limit for preservation prescribed by 18 U.S.C. § 2703(f). Thus, there remains the possibility that relevant content in the account has been deleted.<sup>15</sup> Nevertheless, we consider that possibility remote because, to the FBI's knowledge, in January 2010, neither Mr. Kim nor the Reporter knew that Mr. Kim was a target of this investigation nor that the existence of the [REDACTED]@gmail.com account was known to the FBI. On April 9, 2010, another 90-day extension of the preservation order was permitted by Google, Inc. for the account.

#### IV. COMPUTERS, THE INTERNET, AND E-MAIL

48. I have received training from the FBI related to computer systems and the use of computers during criminal investigations. Based on my education, training and experience, and information provided to me by other law enforcement agents, I know the following:

- (a). The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. The term "computer", as used herein, is defined in 18 U.S.C. § 1030(e)(1) and includes an electronic, magnetic, optical, electrochemical, or

---

<sup>15</sup> On January 21, 2010, Google refused to confirm to an FBI agent whether there is any content in the account without service of formal process.

other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. A computer user accesses the Internet through a computer network or an Internet Service Provider (ISP).

- (b). E-mail, or electronic mail, is a popular method of sending messages and files between computer users. When a computer user sends an e-mail, it is created on the sender's computer, transmitted to the mail server of the sender's e-mail service providers, then transmitted to the mail server of the recipient's e-mail service provider, and eventually transmitted to the recipient's computer. A server is a computer attached to a dedicated network that serves many users. Copies of e-mails are usually maintained on the recipient's e-mail server, and in some cases are maintained on the sender's e-mail server.

49. Based on my training and experience, and information provided to me by other law enforcement agents, I know the following: First, searches of e-mail accounts usually provide information that helps identify the user(s) of the e-mail accounts. Second, individuals who use e-mail in connection with criminal activity, or activity of questionable legality, often set up an e-mail account to be used solely for that purpose. This is often part of an effort to maintain anonymity and to separate personal communication from communication and information that is related to the criminal activity. Third, when the criminal violation involves a conspiracy, a search of an e-mail account often allows the identification of any co-conspirators.

## **V. BACKGROUND REGARDING GOOGLE**

50. Based on my training and experience, I have learned the following about Google:
- (a). Google is an internet services company that, among other things, provides e-mail services (known as gmail). Subscribers obtain an account by registering on the Internet with Google. Google requests subscribers to provide basic information, such as name, gender, zip code and other personal/biographical information. However, Google does not verify the information provided.
  - (b). Google is located at 1600 Amphitheatre Parkway, Mountain View, California. Google maintains electronic records pertaining to the subscribers of its e-mail

services. These records include account access information, e-mail transaction information, and account application information.

- (c). Subscribers to Google may access their Google accounts using the Internet.
- (d). E-mail messages and files sent to a gmail account are stored in the account's "inbox" as long as they are not identified as "SPAM," the account has not exceeded the maximum storage limit, and the account has not been set to forward messages or download to an e-mail client with the option "delete gmail's copy." If the message/file is not deleted by the subscriber, the account is below the maximum storage limit, and the account has not been inactivated, then the message/file will remain on the server indefinitely. E-mail messages and files sent from a gmail account will remain on the server indefinitely unless they are deleted by the subscriber.
- (e). Google provides POP3 access for gmail accounts. POP3 is a protocol by which e-mail client software such as Microsoft Outlook or Netscape Mail can access the servers of an e-mail service provider and download the received messages to a local computer. If POP3 access is enabled, the account user can select to keep a copy of the downloaded messages on the server or to have the messages deleted from the server. The default setting for gmail accounts is to keep a copy of the messages on the server when POP3 access is enabled. Gmail subscribers can also access their accounts through an e-mail client such as Microsoft Outlook by using the IMAP protocol. When gmail subscribers access their accounts through IMAP, a copy of the received messages remains on the server unless explicitly deleted.
- (f). A Google subscriber can store files, including e-mails, text files, and image files, in the subscriber's account on the servers maintained and/or owned by Google.
- (g). E-mails and other files stored by a Google subscriber in a Google account are not necessarily also located on the computer used by the subscriber to access the Google account. The subscriber may store e-mails and other files in their Google account server exclusively. A search of the files in the subscriber's computer will not necessarily uncover the files that the subscriber has stored on the Google server. In addition, communications sent to the Google subscriber by another, but not yet retrieved by the subscriber, will be located on the Google server in the subscriber's account, but not on the computer used by the subscriber.
- (h). Computers located at Google contain information and other stored electronic communications belonging to unrelated third parties. As a federal agent, I am trained and experienced in identifying communications relevant to the crimes under investigation. The personnel of Google are not. I also know that the manner in which the data is preserved and analyzed may be critical to the

successful prosecution of any case based upon this evidence. Computer Forensic Examiners are trained to handle digital evidence. Google employees are not. It would be inappropriate and impractical, however, for federal agents to search the vast computer network of Google for the relevant accounts and then to analyze the contents of those accounts on the premises of Google. The impact on Google's business would be severe.

## **VI. STORED WIRE AND ELECTRONIC COMMUNICATIONS**

51. 18 U.S.C. §§ 2701–2711 is called the “Electronic Communications Privacy Act.”

(a). 18 U.S.C. § 2703(a) provides, in part:

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b). 18 U.S.C. § 2703(b) provides, in part:

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –

(A) Without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or . . . .

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service –

(A) On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission



from), a subscriber or customer of such remote computing service;  
and

(B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

- (c). The Government may also obtain records and other information pertaining to a subscriber or customer of an electronic communication service or remote computing service by way of a search warrant. 18 U.S.C. § 2703(c)(1)(A). No notice to the subscriber or customer is required. 18 U.S.C. § 2703(c)(2).

- (d). 18 U.S.C. § 2711 provides, in part:

As used in this chapter -- (1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and (2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

- (e). 18 U.S.C. § 2510 provides, in part:

(8) "contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;... (14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications; (15) "electronic...communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;... (17) "electronic storage" means - (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

- (f). 18 U.S.C. § 2703(g) provides, in part:

Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

#### **VII. REQUEST FOR NON-DISCLOSURE BY PROVIDER**

52. Pursuant to 18 U.S.C. § 2705(b), this Court can enter an order commanding the PROVIDER not to notify any other person, including the subscriber of the SUBJECT ACCOUNT, of the existence of the warrant because there is reason to believe that notification of the existence of the warrant will result in: (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering of evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardize the investigation. The involvement of the SUBJECT ACCOUNT as set forth above is not public and I know, based on my training and experience, that subjects of criminal investigations will often destroy digital evidence if the subject learns of an investigation. Additionally, if the PROVIDER or other persons notify anyone that a warrant has been issued on the SUBJECT ACCOUNT, the targets of this investigation and other persons may further mask their identity and activity, flee, or otherwise obstruct this investigation. Accordingly, I request that this Court enter an order commanding the PROVIDER not to notify any other person, including the subscriber of the SUBJECT ACCOUNT, of the existence of the warrant.


#### **VIII. REQUEST FOR SEALING**

53. Because this investigation is continuing and disclosure of some of the details of this affidavit may compromise subsequent investigative measures to be taken in this case, may

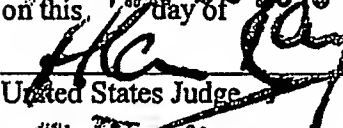

cause subjects to flee, may cause individuals to destroy evidence and/or may otherwise jeopardize this investigation, I respectfully request that this affidavit, and associated materials seeking this search warrant, be sealed until further order of this Court. Finally, I specifically request that the sealing order not prohibit information obtained from this warrant from being shared with other law enforcement and intelligence agencies.

**IX. CONCLUSION**

54. Based on the foregoing, there is probable cause to believe that the Reporter has committed or is committing a violation of 18 U.S.C. § 793 (Unauthorized Disclosure of National Defense Information), as an aider, abettor and/or co-conspirator, and that on the computer systems owned, maintained, and/or operated by Google, Inc., there exists in, and related to, the SUBJECT ACCOUNT, evidence, fruits, and instrumentalities of that violation of section § 793. By this affidavit and application, I request that the Court issue a search warrant directed to Google, Inc., allowing agents to seize the content of the SUBJECT ACCOUNT and other related information stored on the Google servers as further described and delimited in Attachment A hereto.

  
\_\_\_\_\_  
Reginald B. Reyes  
Special Agent  
Federal Bureau of Investigation

Sworn to and subscribed before me  
on this MAY 28 2010  
day of May

  
\_\_\_\_\_  
United States Judge  
  
ALAN KAY  
U.S. MAGISTRATE JUDGE

**ATTACHMENT A: ITEMS TO BE SEIZED**

Pursuant to 18 U.S.C. § 2703 and 42 U.S.C. § 2000aa(a), it is hereby ordered as follows:

**I. SERVICE OF WARRANT AND SEARCH PROCEDURE**

a. Google, Incorporated, a provider of electronic communication and remote computing services, located at 1600 Amphitheatre Parkway, Mountain View, California, (the "PROVIDER") will isolate those accounts and files described in Section II below. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

b. The PROVIDER shall not notify any other person, including the subscriber(s) of [REDACTED]@gmail.com of the existence of the warrant.

c. In order to minimize any disruption of computer service to innocent third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.

d. As soon as practicable after service of this warrant, the PROVIDER shall provide the exact duplicate in electronic form of the account and files described in Section II below and all information stored in that account and files to the following FBI special agent:

Reginald B. Reyes  
FBI-WFO  
601 4<sup>th</sup> Street, NW  
Washington, D.C. 20535  
Fax: 202-278-2864  
Desk: 202-278-4868

The PROVIDER shall send the information to the agent via facsimile and overnight mail, and where maintained in electronic form, on CD-ROM or an equivalent electronic medium.

e. The FBI will make an exact duplicate of the original production from the PROVIDER. The original production from the PROVIDER will be sealed by the FBI and preserved for authenticity and chain of custody purposes.

## **II. FILES AND ACCOUNTS TO BE COPIED BY THE PROVIDER'S EMPLOYEES**

a. Any and all communications, on whatever date, between

██████████@gmail.com ("SUBJECT ACCOUNT") and any of the following accounts:

- (1) ██████████@yahoo.com,
- (2) ██████████@yahoo.com, and
- (3) ██████████@gmail.com.

"Any and all communications" includes, without limitation, received messages (whether "to," "cc'd," or "bcc'd" to the SUBJECT ACCOUNT), forwarded messages, sent messages (whether "to," "cc'd," or "bcc'd" to the three above-listed accounts), deleted messages, and messages maintained in trash or other folders, and any attachments thereto, including videos, documents, photos, internet addresses, and computer files sent to and received from other websites. "Any and all communications" further includes all prior email messages in an email "chain" between the SUBJECT ACCOUNT and any of the three above-listed accounts, whether or not those prior emails were in fact sent between the SUBJECT ACCOUNT and the above-listed accounts;

b. Any and all communications "to" or "from" the SUBJECT ACCOUNT on June 10 and/or June 11, 2009. "Any and all communications" includes, without limitation, received messages (whether "to," "cc'd," or "bcc'd" to the SUBJECT ACCOUNT), forwarded messages, sent messages, deleted messages, messages maintained in trash or other folders, and any attachments thereto, including videos, documents, photos, internet addresses, and computer files

sent to and received from other websites. "Any and all communications" further includes all prior email messages in an email "chain" sent "to" or "from" the SUBJECT ACCOUNT on June 10 or June 11, 2009, whether or not those prior emails in the "chain" were in fact sent or received on June 10 or June 11, 2009;

c. All existing printouts from original storage of all of the electronic mail described above in Section II (a) and II(b);

d. All transactional information of all activity of the SUBJECT ACCOUNT described above in Section II(a) and II(b), including log files, dates, times, methods of connecting, ports, dial-ups, registration Internet Protocol (IP) address and/or locations;

e. All business records and subscriber information, in any form kept, pertaining to the SUBJECT ACCOUNT described above in Section II(a) and II(b), including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, account numbers, screen names, status of accounts, dates of service, methods of payment, telephone numbers, addresses, detailed billing records, and histories and profiles;

f. All records indicating the account preferences and services available to subscribers of the SUBJECT ACCOUNT described above in Section II(a) and II(b).

### **III. INFORMATION TO BE SEIZED BY LAW ENFORCEMENT PERSONNEL**

Items to be seized, which are believed to be evidence and fruits of violations of 18 U.S.C. § 793 (Unauthorized Disclosure of National Defense Information) as follows:

a. The contents of electronic communications, including attachments and stored files, for the SUBJECT ACCOUNT as described and limited by Section II(a) and II(b) above,

including videos, computer files sent to and received from other websites, received messages, sent messages, deleted messages, messages maintained in trash or other folders, any attachments thereto, and all existing printouts from original storage of all of the electronic mail described above in Section II(a) and II(b), that pertain to:

1. records or information related to violations of 18 U.S.C. § 793;
2. any and all communications between Stephen Kim and the author of the article (the "Author") that is the subject matter of the FBI investigation that is the basis for this warrant (the "Article") and any record or information that reflects such communications;
3. records or information relating to Stephen Kim's communications and/or activities on the date of publication of the Article;
4. records or information relating to the Author's communication with any other source or potential source of the information disclosed in the Article;
5. records or information related to Stephen Kim's or the Author's knowledge of laws, regulations, rules and/or procedures prohibiting the unauthorized disclosure of national defense or classified information;
6. records or information related to Stephen Kim's or the Author's knowledge of government rules and/or procedures regarding communications with members of the media;
7. records or information related to any disclosure or prospective disclosure of classified and/or intelligence information;
8. any classified document, image, record or information, and any

communications concerning such documents, images, records, or information;

9. any document, image, record or information concerning the national defense, including but not limited to documents, maps, plans, diagrams, guides, manuals, and other Department of Defense, U.S. military, and/or weapons material, as well as sources and methods of intelligence gathering, and any communications concerning such documents, images, records, or information;
10. records or information related to the state of mind of any individuals seeking the disclosure or receipt of classified, intelligence and/or national defense information;
11. records or information related to the subject matter of the Article; and
12. records or information related to the user(s) of the SUBJECT ACCOUNT.

b. All of the records and information described above in Sections II(d), II(e), and II(f) including:

1. Account information for the SUBJECT ACCOUNT including:
  - (a) Names and associated email addresses;
  - (b) Physical address and location information;
  - (c) Records of session times and durations;
  - (d) Length of service (including start date) and types of service utilized;
  - (e) Telephone or instrument number or other subscriber number or identity,

including any temporarily assigned network address;



(f) The means and source of payment for such service (including any credit card or bank account number); and

(g) Internet Protocol addresses used by the subscriber to register the account or otherwise initiate service.

2. User connection logs for the SUBJECT ACCOUNT for any connections to or from the SUBJECT ACCOUNT. User connection logs should include the following:

- (a) Connection time and date;
- (b) Disconnect time and date;
- (c) Method of connection to system (e.g., SLIP, PPP, Shell);
- (d) Data transfer volume (e.g., bytes);
- (e) The IP address that was used when the user connected to the service,
- (f) Connection information for other systems to which user connected via the SUBJECT ACCOUNT, including:

- (1) Connection destination;
- (2) Connection time and date;
- (3) Disconnect time and date;
- (4) Method of connection to system (e.g., telnet, ftp, http);
- (5) Data transfer volume (e.g., bytes);
- (6) Any other relevant routing information.